

ABSTRACT OF THE DISCLOSURE

A method and architecture for secure transmission of data within optical switched networks. In one embodiment, the optical switched network comprises a photonic burst-switched (PBS) network. Under various schemes, security keys are distributed to each edge node in a PBS network. A source edge node uses an encryption key to encrypt selected data bursts to be sent to a destination edge node via a virtual lightpath coupling the source and destination edge nodes. Security data are embedded in a control burst header indicates to the destination node whether corresponding data bursts sent via the virtual lightpath are encrypted. The security data may also identify an encryption/decryption algorithm and decryption keys to be used. Keys and/or certificates may be generated by or provided to the edge nodes. In some embodiments, public key infrastructure facilities are used in conjunction with employment of private and public keys and certificates.